

Bounds on the Communication Rate Needed to Achieve SK Capacity in the Hypergraphical Source Model

Manuj Mukherjee[†]

Chung Chan[‡]

Navin Kashyap[†]

Qiaoqiao Zhou[‡]

Abstract—In the multiterminal source model of Csiszár and Narayan, the communication complexity, R_{SK} , for secret key (SK) generation is the minimum rate of communication required to achieve SK capacity. An obvious upper bound to R_{SK} is given by R_{CO} , which is the minimum rate of communication required for omniscience. In this paper we derive a better upper bound to R_{SK} for the hypergraphical source model, which is a special instance of the multiterminal source model. The upper bound is based on the idea of fractional removal of hyperedges. It is further shown that this upper bound can be computed in polynomial time. We conjecture that our upper bound is tight. For the special case of a graphical source model, we also give an explicit lower bound on R_{SK} . This bound, however, is not tight, as demonstrated by a counterexample.

I. INTRODUCTION

The problem of secret key (SK) generation for multiple terminals observing i.i.d. sequences of correlated random variables was first studied by Csiszár and Narayan in [1]. The terminals are allowed to communicate *interactively* over a public noiseless channel. After the communication the terminals must agree upon an SK, secured from any eavesdropper having access to the public channel. The *SK capacity*, i.e., the maximum rate of secret key that can be generated was derived in [1]. A quantity of interest in the SK generation problem is the *communication complexity*¹, R_{SK} , which is the minimum rate of communication required to generate an SK of maximum rate.

Tyagi in [2, Theorem 3] has given a complete characterization of R_{SK} for the case of two terminals. Tyagi's arguments have been extended by [3, Theorem 2] to give a lower bound on R_{SK} for the general multiterminal setting. This lower bound was computed and was shown to be tight for a special class of sources in [3, Theorem 6]. However, computing this lower bound for a general multiterminal source remains an open problem. Also, [3] did not provide any discussion on the tightness of this lower bound. Hence, it is useful to derive

upper bounds on R_{SK} . The SK generation protocol in [1] goes through *omniscience*, i.e., all the terminals recovering the entire information of all the other terminals. Thus, the *minimum rate of communication for omniscience*, R_{CO} , is a valid upper bound on R_{SK} .

In this paper, we consider a special case of the multiterminal source model, namely the *hypergraphical source model* studied previously in [5] and [3]. The hypergraphical source model is inspired by the coded co-operative data exchange (CCDE) problem introduced in [6], and has been studied in the context of the “one-shot” SK generation problem, in [7]–[9]. One can also view the hypergraphical source model as a generalization of the pairwise independent network (PIN) model of [10] and [11]. The main contribution of this paper is an upper bound on R_{SK} for the hypergraphical source model. The proof of this upper bound is based on the idea of *decremental SK agreement* studied in [12]. The idea is to keep on removing “randomness” from the hyperedges as long as the SK capacity does not decrease, and then use the R_{CO} of the resulting hypergraph as an upper bound on R_{SK} of the original hypergraph. We further show that the upper bound on R_{SK} thus derived is at least as good as R_{CO} . Computation of this upper bound requires the solution of a linear program, whose separation oracle performs submodular function minimization. As a result the bound is computable in polynomial time. In fact, for the special case when the underlying hypergraph of the source model is a graph, the upper bound reduces to a simple expression. We believe that the upper bound is actually tight. Unfortunately, we do not have a proof of this yet, and therefore we state it as a conjecture. We also give a simple expression for the lower bound on R_{SK} derived in [3, Theorem 2], for sources defined on graphs. Using this expression we are able to construct an example and show that the lower bound in [3] is not tight in general.

We would like to compare and contrast our work with those of Courtade et al. in [8] and [9]. Courtade et al. consider a “one shot” model with each terminal observing only one instance of a random variable. They restrict the communication to linear functions of the source randomness. In [9, Theorem 11], they evaluate the minimum number of bits of communication required to generate a fixed number of bits of SK. It is also shown in [9, Theorem 4] that there exist sources where non-linear communication can strictly outperform any linear communication, in terms of the number

[†]M. Mukherjee and N. Kashyap are with the Department of Electrical Communication Engineering, Indian Institute of Science, Bangalore. Email: {manuj,nkashyap}@ece.iisc.ernet.in.

[‡]C. Chan and Q. Zhou are with the Institute of Network Coding at the Chinese University of Hong Kong. Email: cchan@inc.cuhk.edu.hk, qiaoqiaobupt@gmail.com.

¹Our use of “communication complexity” differs from the use prevalent in the theoretical computer science literature where, following [4], it refers to the total amount of communication, in bits, required to perform some distributed computation.

of bits of communication. On the other hand, our major focus is the asymptotic model involving i.i.d. sequences of correlated random variables at each terminal. We also do not impose any linearity restriction on the communication. However, we consider communication complexity for generating SKs of maximum rate only, contrary to the arbitrary number of bits of SK considered by Courtade et al. It should be mentioned here that the proofs of Courtade et al. proceed by finding “inherently connected subhypergraphs” obtained by completely removing certain hyperedges, as opposed to the “fractional removal” of hyperedges in our proofs. The difference is due to the fact that Courtade et al. consider a one-shot model, whereas we look into an asymptotic scenario. Therefore, restricting ourselves to complete removal of hyperedges only will lead to weaker upper bounds, as demonstrated in Example III.1 appearing later in the paper.

The paper is organized as follows. The basic definitions and concepts are introduced in Section II. Section III presents our main result, an upper bound to R_{SK} . In Section IV, we evaluate the lower bound to R_{SK} stated in [3, Theorem 2], for the special case of graphical source models. The paper concludes with Section V.

II. PRELIMINARIES

In this section we will introduce the major concepts and definitions used in this paper. Throughout, we use \mathbb{N} to denote the set of positive integers. A *weighted hypergraph* is defined by the pair $\mathcal{H} = (\mathcal{M}, \mathbf{w})$ with $\mathcal{M} = \{1, 2, \dots, m\}$ denoting the set of vertices and $\mathbf{w} : 2^{\mathcal{M}} \rightarrow \mathbb{R}^+ \cup \{0\}$ being the weight function on the subsets of the vertices. We will often view \mathbf{w} as a vector whose coordinates are indexed by $e \subseteq \mathcal{M}$. The set of *hyperedges* is obtained from the weight function as the set $\mathcal{E} \triangleq \{e \in 2^{\mathcal{M}} : \mathbf{w}(e) > 0\}$ of subsets of \mathcal{M} with non-zero weights.

We say that a random vector $(X_i : i \in \mathcal{M})$ is a *hypergraphical source* defined on the weighted hypergraph \mathcal{H} if we can write $X_i = (\xi_e : e \in \mathcal{E}, i \in e)$ for some random variables ξ_e 's such that $H(\xi_e) = \mathbf{w}(e)$ and ξ_e 's are mutually independent across $e \in \mathcal{E}$. Whenever \mathcal{E} consists only of subsets e of size 2, we refer to the source as a *graphical source*, and refer to the hyperedges as *edges*.

For the hypergraphical source, \mathcal{M} denotes a set of terminals. Each terminal $i \in \mathcal{M}$ observes n i.i.d. repetitions of a random variable X_i . The n i.i.d. copies of the random variable are denoted by $X_i^n = (\xi_e^n : e \in \mathcal{E}, i \in e)$.² For any subset $A \subseteq \mathcal{M}$, X_A and X_A^n denote the collections of random variables $(X_i : i \in A)$ and $(X_i^n : i \in A)$, respectively. It is easy to check that $H(X_A) = \sum_{e \in \mathcal{E} : e \cap A \neq \emptyset} \mathbf{w}(e)$ and $H(X_A | X_{A^c}) = \sum_{e \in \mathcal{E} : e \subseteq A} \mathbf{w}(e)$.

We point out here that the hypergraphical source model is a special case of the multiterminal source model of [1], which is defined for an arbitrary joint distribution of $X_{\mathcal{M}}$ over a finite support size. Note that the hypergraphical models studied in

[5] and [3] are but a special case of the model studied here, obtained by restricting \mathbf{w} to be integer-valued. If we further restrict $\mathbf{w}(e)$ to take non-zero values only for subsets $e \subseteq \mathcal{M}$ of size 2, we obtain the pairwise independent network (PIN) model of [11].

The terminals communicate through a noiseless public channel, any communication sent through which is accessible to all terminals and to potential eavesdroppers as well. An *interactive communication* is a communication $\mathbf{f} = (f_1, f_2, \dots, f_r)$ with finitely many transmissions f_j , in which any transmission sent by the i th terminal is a deterministic function of X_i^n and all the previous communication, i.e., if terminal i transmits f_j , then f_j is a function only of X_i^n and f_1, \dots, f_{j-1} . We denote the random variable associated with \mathbf{f} by \mathbf{F} ; the support of \mathbf{F} is a finite set \mathcal{F} . The rate of the communication \mathbf{F} is defined as $\frac{1}{n} \log |\mathcal{F}|$. Note that \mathbf{f} , \mathbf{F} and \mathcal{F} implicitly depend on n .

Definition 1. A common randomness (CR) obtained from an interactive communication \mathbf{F} is a sequence of random variables $\mathbf{J}^{(n)}$, $n \in \mathbb{N}$, which are functions of $X_{\mathcal{M}}^n$, such that for any $0 < \epsilon < 1$ and for all sufficiently large n , there exist $J_i = J_i(X_i^n, \mathbf{F})$, $i = 1, 2, \dots, m$, satisfying $\Pr[J_1 = J_2 = \dots = J_m = \mathbf{J}^{(n)}] \geq 1 - \epsilon$.

When $\mathbf{J}^{(n)} = X_{\mathcal{M}}^n$, we say that the terminals in \mathcal{M} have attained *omniscience*. The communication \mathbf{F} which achieves this is called a *communication for omniscience*. It was shown in Proposition 1 of [1] that the minimum rate achievable by a communication for omniscience, denoted by R_{CO} , is equal to

$$\min_{(R_1, R_2, \dots, R_m) \in \mathcal{R}_{\text{CO}}} \sum_{i=1}^m R_i, \text{ where the region } \mathcal{R}_{\text{CO}} \text{ is given by}$$

$$\mathcal{R}_{\text{CO}} = \left\{ (R_i)_{i \in \mathcal{M}} : \sum_{i \in B} R_i \geq \sum_{e \in \mathcal{E} : e \subseteq B} \mathbf{w}(e), B \subsetneq \mathcal{M} \right\}. \quad (1)$$

Henceforth, we will refer to R_{CO} as the “minimum rate of communication for omniscience”. Note that the point (R_1, R_2, \dots, R_m) defined by $R_i = H(X_i)$ for all i lies in \mathcal{R}_{CO} , and hence $R_{\text{CO}} \leq \sum_{i=1}^m H(X_i) < \infty$.

Definition 2. A real number $R \geq 0$ is an achievable SK rate if there exists a CR $\mathbf{K}^{(n)}$, $n \in \mathbb{N}$, obtained from an interactive communication \mathbf{F} satisfying, for any $\epsilon > 0$ and for all sufficiently large n , $I(\mathbf{K}^{(n)}; \mathbf{F}) \leq \epsilon$ and $\frac{1}{n} H(\mathbf{K}^{(n)}) \geq R - \epsilon$. The SK capacity is defined to be the supremum among all achievable rates. The CR $\mathbf{K}^{(n)}$ is called a secret key (SK).

From now on, we will drop the superscript (n) from both $\mathbf{J}^{(n)}$ and $\mathbf{K}^{(n)}$ to keep the notation simple.

The SK capacity can be expressed as [1, Theorem 1]

$$\mathcal{C}(\mathcal{M}) = H(X_{\mathcal{M}}) - R_{\text{CO}}. \quad (2)$$

Other equivalent characterizations of $\mathcal{C}(\mathcal{M})$ exist in the literature. One such characterization of SK capacity can be given via the notion of *multivariate mutual information* defined as follows:

$$I(X_{\mathcal{M}}) \triangleq \min_{\mathcal{P}} I_{\mathcal{P}}(X_{\mathcal{M}}) \quad (3)$$

²Each i.i.d. sequence of random variables ξ_e^n , $e \in \mathcal{E}$, should be thought of as an SK initially shared among the terminals in e .

with $I_{\mathcal{P}}(X_{\mathcal{M}}) \triangleq \frac{1}{|\mathcal{P}|-1} [\sum_{A \in \mathcal{P}} H(X_A) - H(X_{\mathcal{M}})]$ and the minimum being taken over all partitions $\mathcal{P} = \{A_1, A_2, \dots, A_\ell\}$ of \mathcal{M} , of size $\ell \geq 2$. Note that $I(X_{\mathcal{M}}^n) = nI(X_{\mathcal{M}})$. The quantity $I(X_{\mathcal{M}})$ is a generalization of the mutual information to a multiterminal setting; indeed, for $m = 2$, we have $I(X_1, X_2) = I(X_1; X_2)$. It was shown in Theorem 1.1 of [5] and Theorem 4.1 of [13] that

$$\mathcal{C}(\mathcal{M}) = I(X_{\mathcal{M}}). \quad (4)$$

For the rest of this paper we shall use $\mathcal{C}(\mathcal{M})$ and $I(X_{\mathcal{M}})$ interchangeably.

We will denote by \mathcal{P}^* the finest partition that achieves the minimum in (3). Theorem 5.2 of [13] guarantees that \mathcal{P}^* exists and is unique, and will henceforth be referred to as the *fundamental partition*. In particular, we call the partition $\{\{1\}, \{2\}, \dots, \{m\}\}$ consisting of m singleton cells as the *singleton partition* and denote it by \mathcal{S} . The sources satisfying $\mathcal{P}^* = \mathcal{S}$ will be referred to as *Type \mathcal{S} sources*.

We are now in a position to make the notion of communication complexity rigorous.

Definition 3. A real number $R \geq 0$ is said to be an achievable rate of interactive communication for maximal-rate SK if for all $\epsilon > 0$ and for all sufficiently large n , there exist (i) an interactive communication \mathbf{F} satisfying $\frac{1}{n} \log |\mathcal{F}| \leq R + \epsilon$, and (ii) an SK \mathbf{K} obtained from \mathbf{F} such that $\frac{1}{n} H(\mathbf{K}) \geq I(X_{\mathcal{M}}) - \epsilon$.

The infimum among all such achievable rates is called the communication complexity of achieving SK capacity, denoted by R_{SK} .

The proof of Theorem 1 in [1] shows that there exists an interactive communication \mathbf{F} that enables omniscience at all terminals and from which a maximal-rate SK can be obtained. Therefore, we have $R_{\text{SK}} \leq R_{\text{CO}} < \infty$. Hence, in terms of communication complexity, the sources that satisfy $R_{\text{SK}} = R_{\text{CO}}$ are the worst-case sources. We will henceforth refer to them as *R_{SK} -maximal sources*. Such sources do exist, as shown in Section VI of [3].

III. UPPER BOUND ON R_{SK}

In this section we derive an upper bound on R_{SK} based on the notion of *decremental SK agreement* studied in [12]. The idea is to “fractionally remove” hyperedges from the original hypergraph. To be precise, consider a hypergraphical source $X_{\mathcal{M}}$ defined on the weighted hypergraph $\mathcal{H} = (\mathcal{M}, \mathbf{w})$. A non-negative vector \mathbf{x} satisfying $\mathbf{x} \leq \mathbf{w}$ (coordinatewise) is called a *fractional packing* of the hypergraph \mathcal{H} . For any fractional packing \mathbf{x} , define a new hypergraphical source on the weighted hypergraph $\mathcal{H}^{\mathbf{x}} = (\mathcal{M}, \mathbf{x})$. Observe that since $\mathbf{x} \leq \mathbf{w}$, the source defined on $\mathcal{H}^{\mathbf{x}}$ is obtained by “removing” some randomness from $X_{\mathcal{M}}$.

We denote the relevant quantities for the source defined on $\mathcal{H}^{\mathbf{x}}$ by adding a superscript \mathbf{x} to the original notation. For example, we use $X_{\mathcal{M}}^{\mathbf{x}}$, $R_{\text{CO}}^{\mathbf{x}}$, $R_{\text{SK}}^{\mathbf{x}}$ etc. It is easy to see that $I(X_{\mathcal{M}}^{\mathbf{x}}) \leq I(X_{\mathcal{M}})$, since any SK generation protocol for $X_{\mathcal{M}}^{\mathbf{x}}$ is also a valid SK generation protocol for $X_{\mathcal{M}}$.

To proceed, we need to introduce some notation. Define the set Γ to be the set of all fractional packings \mathbf{x} , satisfying the following constraints:

$$\mathbf{x} \leq \mathbf{w}, \quad (5)$$

$$\exists \mathbf{r} = (r_i)_{i \in \mathcal{M}} \text{ such that } \sum_{i \in B} r_i \geq \sum_{e \in \mathcal{E}: e \subseteq B} \mathbf{x}(e), \forall B \subsetneq \mathcal{M}, \quad (6)$$

$$\sum_{e \in \mathcal{E}} \mathbf{x}(e) - \sum_{i=1}^m r_i = I(X_{\mathcal{M}}). \quad (7)$$

Note that Γ is non-empty since $\mathbf{w} \in \Gamma$. This follows immediately by choosing $(r_1, r_2, \dots, r_m) \in \mathcal{R}_{\text{CO}}$ that achieves R_{CO} and by noting (2) and the fact that $H(X_{\mathcal{M}}) = \sum_{e \in \mathcal{E}} \mathbf{w}(e)$. Denote by Γ^* the set of fractional packings \mathbf{x} satisfying $I(X_{\mathcal{M}}^{\mathbf{x}}) = I(X_{\mathcal{M}})$, i.e., the fractional packing \mathbf{x} does not decrease the SK capacity. It is easy to see that $\mathbf{w} \in \Gamma^*$, and hence it is non-empty.

We now state the upper bound to R_{SK} in the following theorem.

Theorem 1. For a hypergraphical source model $X_{\mathcal{M}}$ defined on the weighted hypergraph $\mathcal{H} = (\mathcal{M}, \mathbf{w})$ we have

$$R_{\text{SK}} \leq \sum_{e \in \mathcal{E}} \mathbf{x}^*(e) - I(X_{\mathcal{M}}),$$

where \mathbf{x}^* is an optimal solution for the linear program $\min \sum_{e \in \mathcal{E}} \mathbf{x}(e)$ subject to the constraints $\mathbf{x} \in \Gamma$.

Since, $\mathbf{x}^* \leq \mathbf{w}$, by (2) we have that the upper bound in Theorem 1 is at least as good as R_{CO} . We will need the following lemma in order to prove Theorem 1.

Lemma 2. For a hypergraphical source $X_{\mathcal{M}}$ defined on the weighted hypergraph $\mathcal{H} = (\mathcal{M}, \mathbf{w})$ we have

$$\Gamma = \Gamma^*.$$

Proof: To begin with note that $H(X_{\mathcal{M}}^{\mathbf{x}}) = \sum_{e \in \mathcal{E}} \mathbf{x}(e)$. It is straightforward to see that the constraints in (6) are nothing but the \mathcal{R}_{CO} constraints of (1) for the source defined on $\mathcal{H}^{\mathbf{x}}$. Therefore, the constraint (7) along with (2) shows that a fractional packing $\mathbf{x} \in \Gamma$ does not decrease the SK capacity, and so $\mathbf{x} \in \Gamma^*$. Therefore, $\Gamma \subseteq \Gamma^*$.

On the other hand, any fractional packing $\mathbf{x} \in \Gamma^*$ does not decrease the SK capacity. Hence, by (2), there exists a rate point \mathbf{r} satisfying the \mathcal{R}_{CO} constraints, i.e., the constraints in (6), as well as the constraint (7). So, $\mathbf{x} \in \Gamma$ and hence $\Gamma^* \subseteq \Gamma$, which completes the proof. ■

We are now in a position to prove Theorem 1.

Proof of Theorem 1: To begin with, consider any $\mathbf{x} \in \Gamma$. By Lemma 2, we also have that $\mathbf{x} \in \Gamma^*$. Since any SK generation protocol for $X_{\mathcal{M}}^{\mathbf{x}}$ is also a valid SK generation protocol for $X_{\mathcal{M}}$, the fact that $I(X_{\mathcal{M}}^{\mathbf{x}}) = I(X_{\mathcal{M}})$ implies that $R_{\text{SK}} \leq R_{\text{SK}}^{\mathbf{x}} \leq R_{\text{CO}}^{\mathbf{x}}$. Using (2), we have $R_{\text{CO}}^{\mathbf{x}} = H(X_{\mathcal{M}}^{\mathbf{x}}) - I(X_{\mathcal{M}}^{\mathbf{x}}) = \sum_{e \in \mathcal{E}} \mathbf{x}(e) - I(X_{\mathcal{M}})$. Therefore, combining the above results we have for any $\mathbf{x} \in \Gamma$, $R_{\text{SK}} \leq \sum_{e \in \mathcal{E}} \mathbf{x}(e) - I(X_{\mathcal{M}})$. In order to get the best upper bound we simply choose \mathbf{x}^* which minimizes $\sum_{e \in \mathcal{E}} \mathbf{x}(e)$ among all possible $\mathbf{x} \in \Gamma$. ■

Before proceeding, we provide an example where we explicitly evaluate the upper bound in Theorem 1.

Example III.1. Consider the hypergraph $\mathcal{H} = (\mathcal{M}, \mathbf{w})$, with $|\mathcal{M}| = 4$ and weight vector \mathbf{w} given as follows:

$$\begin{aligned} \mathbf{w}(e) &= 1, e = \{1, 4\}, \{2, 3\}, \{3, 4\} \\ &= 2, e = \{1, 2\} \\ &= 0, \text{ otherwise.} \end{aligned}$$

One can easily check that $\mathcal{P}^* = \{\{1, 2\}, \{3\}, \{4\}\}$, $I(X_{\mathcal{M}}) = 1.5$ and $R_{CO} = 3.5$. Solving the linear program in Theorem 1, we see that the optimal fractional packing \mathbf{x}^* is given by $\mathbf{x}^*(\{1, 2\}) = 1.5$ and $\mathbf{x}^*(e) = \mathbf{w}(e)$ for all $e \neq \{1, 2\}$. Thus, Theorem 1 gives the upper bound $R_{SK} \leq 3 < R_{CO}$.

It is not difficult to check that no integer-valued $\mathbf{x} \neq \mathbf{w}$ is possible without decreasing the SK capacity. Thus even if \mathbf{w} is integer-valued, removing a hyperedge by an integer amount or completely need not be optimal, and fractional removal is a better thing to do.

We now turn our attention to evaluating the upper bound in Theorem 1. Evaluating the upper bound in Theorem 1 requires the knowledge of $I(X_{\mathcal{M}})$, which in turn can be calculated in strongly polynomial time as shown in [13]. Knowing $I(X_{\mathcal{M}})$, the upper bound in Theorem 1 can be computed in polynomial time. This is because the separation oracle for the constraints in (6), i.e., $\sum_{i \in B} r_i \geq \sum_{e \in \mathcal{E}: e \subseteq B} \mathbf{x}(e) = H(X_B^{\mathbf{x}} | X_{B^c}^{\mathbf{x}})$, for all $B \subsetneq \mathcal{M}$, is but an instance of a submodular function minimization given by $\min_{B \subsetneq \mathcal{M}} \left\{ \sum_{i \in B} r_i - H(X_B^{\mathbf{x}} | X_{B^c}^{\mathbf{x}}) \right\} \geq 0$. The fact that submodular function minimization can be carried out in polynomial time (see Theorem 45.1 of [14]), implies that the upper bound in Theorem 1 can also be computed in polynomial time (see Theorem 5.10 of [14]).

It turns out that for the special case of graphical models, i.e., when \mathcal{E} consists only of sets of size 2, the upper bound in Theorem 1 reduces to a very simple expression.

Theorem 3. For a source $X_{\mathcal{M}}$ defined on a weighted graph $\mathcal{G} = (\mathcal{M}, \mathbf{w})$ we have

$$R_{SK} \leq (m-2)I(X_{\mathcal{M}}).$$

Before proceeding, observe that for a graphical model, we have

$$I_{\mathcal{P}}(X_{\mathcal{M}}) = \frac{1}{|\mathcal{P}|-1} \sum_{e \in \mathcal{E}_{\mathcal{P}}} \mathbf{w}(e), \quad (8)$$

where $\mathcal{E}_{\mathcal{P}}$ denotes the set of edges $e \in \mathcal{E}$ which are not contained in any parts of the partition \mathcal{P} . We require the following lemma to prove Theorem 1.

Lemma 4. For a source $X_{\mathcal{M}}$ defined on the graph $\mathcal{G} = (\mathcal{M}, \mathbf{w})$, we have $\Gamma = \Gamma^* = \{\mathbf{w}\}$ only if $X_{\mathcal{M}}$ is Type \mathcal{S} .

Proof: We shall prove the lemma by contradiction. Suppose that $\Gamma = \{\mathbf{w}\}$ but $\mathcal{P}^* \neq \mathcal{S}$. We will show that there exists a fractional packing $\mathbf{x} \neq \mathbf{w}$ which lies in Γ , thereby contradicting the assumption $\mathcal{P}^* \neq \mathcal{S}$.

We first prove that for every $A \in \mathcal{P}^*$ with $|A| \geq 2$, there exists at least one edge of \mathcal{G} contained in A . Otherwise, any refinement of \mathcal{P}^* to some $\tilde{\mathcal{P}}$ by arbitrarily splitting A into two parts will satisfy $\mathcal{E}_{\tilde{\mathcal{P}}} = \mathcal{E}_{\mathcal{P}^*}$, and hence, $\sum_{e \in \mathcal{E}_{\tilde{\mathcal{P}}}} \mathbf{w}(e) =$

$\sum_{e \in \mathcal{E}_{\mathcal{P}^*}} \mathbf{w}(e)$. That would imply $I_{\mathcal{P}^*}(X_{\mathcal{M}}) > I_{\tilde{\mathcal{P}}}(X_{\mathcal{M}})$, violating the optimality of \mathcal{P}^* in (3). Hence, we can fix a $\tilde{e} \subseteq A$.

Next we obtain a fractional packing $\mathbf{x} \neq \mathbf{w}$ by removing randomness from \tilde{e} . Let $\epsilon = \min_{\mathcal{P} \neq \mathcal{P}^*} (I_{\mathcal{P}}(X_{\mathcal{M}}) - I_{\mathcal{P}^*}(X_{\mathcal{M}}))$, the minimum being taken over all partitions $\mathcal{P} \neq \mathcal{P}^*$ which are not coarser versions of \mathcal{P}^* . \mathcal{P}^* being the fundamental partition (and $\mathcal{P}^* \neq \mathcal{S}$) we have $\epsilon > 0$; choose $0 < \delta < \epsilon$. We claim that the fractional packing \mathbf{x} , defined by $\mathbf{x}(\tilde{e}) = \mathbf{w}(\tilde{e}) - \delta$, and $\mathbf{x}(e) = \mathbf{w}(e)$, for all $e \neq \tilde{e}$, lies in Γ . This will violate the fact that $\Gamma = \{\mathbf{w}\}$ and hence we will have the result by contradiction. To complete the proof we require to show that $\mathbf{x} \in \Gamma (= \Gamma^*)$.

To proceed, consider the graph $\mathcal{G}^{\mathbf{x}}$. Observe that by (8), $I_{\mathcal{P}^*}(X_{\mathcal{M}}^{\mathbf{x}}) = I_{\mathcal{P}^*}(X_{\mathcal{M}})$ and hence $I_{\mathcal{P}^*}(X_{\mathcal{M}}^{\mathbf{x}}) = I(X_{\mathcal{M}})$. For any partition $\tilde{\mathcal{P}}$ which is a coarser version of \mathcal{P}^* , we have $I_{\tilde{\mathcal{P}}}(X_{\mathcal{M}}^{\mathbf{x}}) = I_{\tilde{\mathcal{P}}}(X_{\mathcal{M}}) \geq I(X_{\mathcal{M}})$, using (8). On the other hand, consider any partition \mathcal{P}' which is not \mathcal{P}^* or a coarser version of it. By the choice of \mathbf{x} we have, $\sum_{e \in \mathcal{E}_{\mathcal{P}'}} \mathbf{x}(e) \geq \sum_{e \in \mathcal{E}_{\mathcal{P}'}} \mathbf{w}(e) - \delta$.

Thus, using (8) we have, $I_{\mathcal{P}'}(X_{\mathcal{M}}^{\mathbf{x}}) \geq \frac{1}{|\mathcal{P}'|-1} \left[\sum_{e \in \mathcal{E}_{\mathcal{P}'}} \mathbf{w}(e) - \delta \right] \geq I_{\mathcal{P}'}(X_{\mathcal{M}}) - \delta > I_{\mathcal{P}'}(X_{\mathcal{M}}) - \epsilon \geq I(X_{\mathcal{M}})$. Hence, by (3), we have $I(X_{\mathcal{M}}^{\mathbf{x}}) \geq I(X_{\mathcal{M}})$. Since $I(X_{\mathcal{M}}^{\mathbf{x}}) \leq I(X_{\mathcal{M}})$ always holds, the result follows. ■

We now prove Theorem 3.

Proof of Theorem 3: We first show that the source $X_{\mathcal{M}}^*$ defined on the weighted graph $\mathcal{G}^{\mathbf{x}^*}$ is Type \mathcal{S} . If not, Lemma 4 will imply that there exists a fractional packing $\mathbf{x}' \leq \mathbf{x}^*$ of $(\mathcal{M}, \mathbf{x}^*)$, satisfying $I(X_{\mathcal{M}}^{\mathbf{x}'}) = I(X_{\mathcal{M}}^{\mathbf{x}^*}) = I(X_{\mathcal{M}})$. This in turn implies that $\mathbf{x}' \in \Gamma^* = \Gamma$, thereby violating the optimality of \mathbf{x}^* . Hence, $X_{\mathcal{M}}^*$ is Type \mathcal{S} . As a result we have, $I(X_{\mathcal{M}}) = I(X_{\mathcal{M}}^*) = I_{\mathcal{S}}(X_{\mathcal{M}}^*) = \frac{1}{m-1} \sum_{e \in \mathcal{E}} \mathbf{x}^*(e)$.

Therefore, the bound in Theorem 1 reduces to $(m-2)I(X_{\mathcal{M}})$ as required. ■

We would like to remark here that for the special case of PIN models on graphs, which is obtained by restricting \mathbf{w} in the graphical model to be integer-valued, the same upper bound was also derived in Lemma 9 of [3], using protocols for SK generation developed in [11] based on *spanning tree packing*.

It was shown in the proof of Theorem 3 that the source $X_{\mathcal{M}}^*$ is Type \mathcal{S} . Therefore, Theorem 6 of [3] shows that $X_{\mathcal{M}}^*$ is R_{SK} -maximal. As a result, we have using Theorem 3 and (2) that $R_{SK}^* = (m-2)I(X_{\mathcal{M}})$. Since $X_{\mathcal{M}}^*$ was obtained from $X_{\mathcal{M}}$ by throwing away some randomness that did not affect the SK capacity, we believe that it should not affect R_{SK} as well. Hence, we conjecture that the upper bound in Theorem 3 is tight. In fact, this leads us to believe that the upper bound

in Theorem 1 is tight which is stated as a conjecture below.

Conjecture. *The upper bounds in Theorems 1 and 3 are tight.*

IV. LOWER BOUNDS ON R_{SK}

In this section, we restrict our attention to source models defined on graphs only and show that the lower bound derived in Theorem 2 of [3] reduces to a very simple expression. For the hypergraphical model in its full generality computing that bound is difficult, except for the special case of Type \mathcal{S} sources on t -uniform hypergraphs as shown in Theorem 6 of [3].

Theorem 5. *For a source $X_{\mathcal{M}}$ defined on a weighted graph $\mathcal{G} = (\mathcal{M}, \mathbf{w})$ we have*

$$R_{SK} \geq \frac{|\mathcal{P}^*| - 2}{|\mathcal{P}^*| - 1} \sum_{e \in \mathcal{E}_{\mathcal{P}^*}} \mathbf{w}(e),$$

where $\mathcal{E}_{\mathcal{P}^*} \subseteq \mathcal{E}$ denotes the set of edges not contained within any of the cells of the partition \mathcal{P}^* .

To prove this theorem we need to introduce some definitions and results from [3]. We begin by introducing the definition of *conditional multivariate mutual information*, which is a generalization of conditional mutual information to the multiterminal setting. The conditional multivariate mutual information of $X_{\mathcal{M}}$ given a random variable \mathbf{L} is defined as³

$$I(X_{\mathcal{M}}|\mathbf{L}) \triangleq \frac{1}{|\mathcal{P}^*| - 1} \left[\sum_{A \in \mathcal{P}^*} H(X_A|\mathbf{L}) - H(X_{\mathcal{M}}|\mathbf{L}) \right]. \quad (9)$$

The definition of $I(X_{\mathcal{M}}|\mathbf{L})$ applies to any collection of jointly distributed random variables $X_{\mathcal{M}}$; in particular it applies to the collection $X_{\mathcal{M}}^n$. To be clear,

$$I(X_{\mathcal{M}}^n|\mathbf{L}) \triangleq \frac{1}{|\mathcal{P}^*| - 1} \left[\sum_{A \in \mathcal{P}^*} H(X_A^n|\mathbf{L}) - H(X_{\mathcal{M}}^n|\mathbf{L}) \right].$$

We use this definition of $I(X_{\mathcal{M}}|\mathbf{L})$ to extend to the multiterminal setting an asymptotic version of two-terminal Wyner common information (see [15]) appearing in [2].⁴

Definition 4. *A (multiterminal) Wyner common information (CI_W) for $X_{\mathcal{M}}$ is a sequence of finite-valued functions $\mathbf{L}^{(n)} = \mathbf{L}^{(n)}(X_{\mathcal{M}}^n)$ such that $\frac{1}{n}I(X_{\mathcal{M}}^n|\mathbf{L}^{(n)}) \rightarrow 0$ as $n \rightarrow \infty$. An interactive common information (CI) for $X_{\mathcal{M}}$ is a Wyner common information of the form $\mathbf{L}^{(n)} = (\mathbf{J}, \mathbf{F})$, where \mathbf{F} is an interactive communication and \mathbf{J} is a CR obtained from \mathbf{F} .*

Similar to Definitions 1 and 2 we shall drop the superscript (n) from $\mathbf{L}^{(n)}$ for notational simplicity. Wyner common informations \mathbf{L} do exist: for example, the identity map $\mathbf{L} = X_{\mathcal{M}}$ is a CI_W . To see that CIs (\mathbf{J}, \mathbf{F}) also exist, observe that $\mathbf{J} = X_{\mathcal{M}}$ and a communication \mathbf{F} enabling omniscience constitute a CI_W , and hence, a CI.

³It should be noted that the definition of conditional multivariate mutual information used here is slightly different from what we called “conditional multipartite information” in [3]. However, the main results of all of these works continue to hold even with the current definition.

⁴One possible generalization of the non-asymptotic Wyner common information appearing in [15] to the multiterminal setting is carried out in [16].

Definition 5. *A real number $R \geq 0$ is an achievable CI_W (resp. CI) rate if there exists a CI_W \mathbf{L} (resp. a CI $\mathbf{L} = (\mathbf{J}, \mathbf{F})$) such that for all $\epsilon > 0$, we have $\frac{1}{n}H(\mathbf{L}) \leq R + \epsilon$ for all sufficiently large n . We denote the infimum among all achievable CI_W (resp. CI) rates by $CI_W(X_{\mathcal{M}})$ (resp. $CI(X_{\mathcal{M}})$).*

With these definitions in hand, we summarize some of the results of [3] needed for this section in the following theorem.

Theorem 6. *For a source $X_{\mathcal{M}}$, we have*

$$I(X_{\mathcal{M}}) \leq CI_W(X_{\mathcal{M}}) \leq CI(X_{\mathcal{M}}) \leq H(X_{\mathcal{M}}),$$

and

$$R_{SK} \geq CI(X_{\mathcal{M}}) - I(X_{\mathcal{M}}).$$

To proceed, we will need a variant of the Lemma 7 of [3] for graphs.

Lemma 7. *For any function \mathbf{L} of a source $X_{\mathcal{M}}^n$ defined on a weighted graph $\mathcal{G} = (\mathcal{M}, \mathbf{w})$ with fundamental partition \mathcal{P}^* , we have*

$$\sum_{A \in \mathcal{P}^*} I(X_A^n; \mathbf{L}) \leq 2H(\mathbf{L}).$$

The proof follows on the lines of Lemma 7 of [3] and can be found in Appendix A. The following lemma determines the minimum rate of interactive common information $CI(X_{\mathcal{M}})$ for graphical models.

Lemma 8. *For the source $X_{\mathcal{M}}$ defined on a weighted graph $\mathcal{G} = (\mathcal{M}, \mathbf{w})$, with fundamental partition \mathcal{P}^* , we have*

$$CI(X_{\mathcal{M}}) = \sum_{e \in \mathcal{E}_{\mathcal{P}^*}} \mathbf{w}(e).$$

Proof: To begin with, we observe that it suffices to prove that $CI_W(X_{\mathcal{M}}) = \sum_{e \in \mathcal{E}_{\mathcal{P}^*}} \mathbf{w}(e)$. Indeed, consider \mathbf{F} to be a broadcast of all the random variables ξ_e^n associated with the edges in $e \in \mathcal{E}_{\mathcal{P}^*}$. Let $\mathbf{J} = (\xi_e^n : e \in \mathcal{E}_{\mathcal{P}^*})$. It is straightforward to verify that $I(X_{\mathcal{M}}^n|\mathbf{J}, \mathbf{F}) = 0$, since $\sum_{A \in \mathcal{P}^*} H(X_A^n|\mathbf{J}, \mathbf{F}) = H(X_{\mathcal{M}}^n|\mathbf{J}, \mathbf{F}) = \sum_{e \notin \mathcal{E}_{\mathcal{P}^*}} \mathbf{w}(e)$. Therefore, the pair (\mathbf{J}, \mathbf{F}) constitutes a CI whose rate is $\sum_{e \in \mathcal{E}_{\mathcal{P}^*}} \mathbf{w}(e)$. Hence, we would have $CI(X_{\mathcal{M}}) \leq \sum_{e \in \mathcal{E}_{\mathcal{P}^*}} \mathbf{w}(e) = CI_W(X_{\mathcal{M}})$, which along with Theorem 6 would give the result.

The proof of $CI_W(X_{\mathcal{M}}) = \sum_{e \in \mathcal{E}_{\mathcal{P}^*}} \mathbf{w}(e)$ follows along the lines of the proof of Theorem 6 of [3]. At first choosing $\mathbf{L} = (\xi_e^n : e \in \mathcal{E}_{\mathcal{P}^*})$, it follows immediately that $I(X_{\mathcal{M}}^n|\mathbf{L}) = 0$. Thus, \mathbf{L} is a CI_W for $X_{\mathcal{M}}^n$, and so $CI_W(X_{\mathcal{M}}) \leq \sum_{e \in \mathcal{E}_{\mathcal{P}^*}} \mathbf{w}(e)$. Next, we prove $CI_W(X_{\mathcal{M}}) \geq \sum_{e \in \mathcal{E}_{\mathcal{P}^*}} \mathbf{w}(e)$. To proceed, let \mathbf{L} be any function of $X_{\mathcal{M}}^n$. Then, we have

$$\begin{aligned} I(X_{\mathcal{M}}^n|\mathbf{L}) &= \frac{1}{|\mathcal{P}^*| - 1} \left[\sum_{A \in \mathcal{P}^*} H(X_A^n|\mathbf{L}) - H(X_{\mathcal{M}}^n|\mathbf{L}) \right] \\ &= \frac{1}{|\mathcal{P}^*| - 1} \left[\sum_{A \in \mathcal{P}^*} (H(X_A^n, \mathbf{L}) - H(\mathbf{L})) \right. \\ &\quad \left. - H(X_{\mathcal{M}}^n, \mathbf{L}) + H(\mathbf{L}) \right] \end{aligned}$$

$$\begin{aligned}
&= H(X_{\mathcal{M}}^n, \mathbf{L}) - H(\mathbf{L}) \\
&\quad + \frac{1}{|\mathcal{P}^*|-1} \left[\sum_{A \in \mathcal{P}^*} (H(X_A^n, \mathbf{L}) - H(X_{\mathcal{M}}^n, \mathbf{L})) \right] \\
&= H(X_{\mathcal{M}}^n) - H(\mathbf{L}) - \frac{1}{|\mathcal{P}^*|-1} \sum_{A \in \mathcal{P}^*} H(X_A^n | X_{\mathcal{M}}^n, \mathbf{L}) \tag{10}
\end{aligned}$$

$$\begin{aligned}
&= H(X_{\mathcal{M}}^n) - H(\mathbf{L}) \\
&\quad - \frac{1}{|\mathcal{P}^*|-1} \sum_{A \in \mathcal{P}^*} \left[H(X_{\mathcal{M}}^n) - H(X_A^n) - H(\mathbf{L} | X_A^n) \right] \tag{11}
\end{aligned}$$

$$\begin{aligned}
&= n \sum_{e \in \mathcal{E}} \mathbf{w}(e) \left(1 - \frac{|\mathcal{P}^*|}{|\mathcal{P}^*|-1} \right) \\
&\quad + \frac{n}{|\mathcal{P}^*|-1} \left[\sum_{e \in \mathcal{E}} \mathbf{w}(e) + \sum_{e \in \mathcal{E}_{\mathcal{P}^*}} \mathbf{w}(e) \right] - H(\mathbf{L}) \\
&\quad + \frac{1}{|\mathcal{P}^*|-1} \sum_{A \in \mathcal{P}^*} H(\mathbf{L} | X_A^n) \tag{12}
\end{aligned}$$

$$\begin{aligned}
&= \frac{n}{|\mathcal{P}^*|-1} \sum_{e \in \mathcal{E}_{\mathcal{P}^*}} \mathbf{w}(e) \\
&\quad - \frac{1}{|\mathcal{P}^*|-1} \left[\sum_{A \in \mathcal{P}^*} I(X_A^n; \mathbf{L}) - H(\mathbf{L}) \right] \\
&= \frac{n}{|\mathcal{P}^*|-1} \left(\sum_{e \in \mathcal{E}_{\mathcal{P}^*}} \mathbf{w}(e) - \frac{1}{n} H(\mathbf{L}) \right) \\
&\quad - \frac{1}{|\mathcal{P}^*|-1} \left[\sum_{A \in \mathcal{P}^*} I(X_A^n; \mathbf{L}) - 2H(\mathbf{L}) \right] \\
&\geq \frac{n}{|\mathcal{P}^*|-1} \left(\sum_{e \in \mathcal{E}_{\mathcal{P}^*}} \mathbf{w}(e) - \frac{1}{n} H(\mathbf{L}) \right), \tag{13}
\end{aligned}$$

where (10) and (11) follow from the fact that \mathbf{L} is a function of $X_{\mathcal{M}}^n$; (12) follows from the fact that $H(X_{\mathcal{M}}^n) = n \sum_{e \in \mathcal{E}} \mathbf{w}(e)$ and $\sum_{A \in \mathcal{P}^*} H(X_A^n) = n \left[\sum_{e \in \mathcal{E}} \mathbf{w}(e) + \sum_{e \in \mathcal{E}_{\mathcal{P}^*}} \mathbf{w}(e) \right]$; and (13) is due to Lemma 7.

Now, consider \mathbf{L} to be any CI_W so that for any $\epsilon > 0$, we have $\frac{1}{n} I(X_{\mathcal{M}}^n | \mathbf{L}) < \frac{\epsilon}{(|\mathcal{P}^*|-1)}$ for all sufficiently large n . The bound in (13) thus yields $\frac{1}{n} H(\mathbf{L}) > \sum_{e \in \mathcal{E}_{\mathcal{P}^*}} \mathbf{w}(e) - \epsilon$ for all sufficiently large n . Hence, it follows that $\text{CI}_W(X_{\mathcal{M}}) \geq \sum_{e \in \mathcal{E}_{\mathcal{P}^*}} \mathbf{w}(e)$. Therefore, we obtain $\text{CI}_W(X_{\mathcal{M}}) = \sum_{e \in \mathcal{E}_{\mathcal{P}^*}} \mathbf{w}(e)$. ■

We now prove Theorem 5.

Proof of Theorem 5: For the source $X_{\mathcal{M}}$ we have

$$R_{\text{SK}} \geq \text{CI}(X_{\mathcal{M}}) - I(X_{\mathcal{M}}) \tag{14}$$

$$\begin{aligned}
&= \sum_{e \in \mathcal{E}_{\mathcal{P}^*}} \mathbf{w}(e) - \frac{1}{|\mathcal{P}^*|-1} \sum_{e \in \mathcal{E}_{\mathcal{P}^*}} \mathbf{w}(e) \tag{15} \\
&= \frac{|\mathcal{P}^*|-2}{|\mathcal{P}^*|-1} \sum_{e \in \mathcal{E}_{\mathcal{P}^*}} \mathbf{w}(e)
\end{aligned}$$

where, (14) follows from Theorem 6 and (15) follows from

Lemma 8. ■

Unfortunately, it turns out that the lower bound in Theorem 5 is not tight in general as illustrated by the following example.

Example IV.1. Consider the source $X_{\mathcal{M}}$ defined on a weighted graph $\mathcal{G} = (\mathcal{M}, \mathbf{w})$ with $|\mathcal{M}| = 4$. The weight vector \mathbf{w} is given by $\mathbf{w}(e) = 1$ for $e = \{1, 2\}, \{1, 3\}, \{2, 3\}$ and $\{3, 4\}$, and $\mathbf{w}(e) = 0$ otherwise. Thus, $\mathcal{E} = \{\{1, 2\}, \{1, 3\}, \{2, 3\}, \{3, 4\}\}$. It is straightforward to verify that $\mathcal{P}^* = \{\{1, 2, 3\}, \{4\}\}$ and $I(X_{\mathcal{M}}) = 1$. Theorem 5 gives the lower bound $R_{\text{SK}} \geq 0$ for this source. However, it is clear that the combined observations of terminal 1 and 2, i.e., $X_{\{1,2\}}^n$, is completely independent of X_4^n . Hence, a communication of positive rate would certainly be required for achieving SK capacity. Thus, $R_{\text{SK}} > 0$, which implies that the lower bound in Theorem 5 is loose.

V. CONCLUDING REMARKS

The upper bound in Theorem 1 is the first reported upper bound on R_{SK} for any instance of the multiterminal source model of [1]. We showed that this bound is at least as good as the obvious upper bound of R_{CO} , and can in fact be stronger as illustrated by Example III.1. We further show that this upper bound can be computed in polynomial time. We believe that this upper bound is tight. Due to the lack of a proof we have left it as a conjecture. We have also evaluated the lower bound on R_{SK} stated in [3, Theorem 2] for the special case of graphical source models. The evaluation enabled us to construct an example showing that the lower bound is not tight in general.

ACKNOWLEDGEMENTS

The authors would like to thank Navid Nouri for stimulating discussions which helped in writing this paper and gain a better understanding of the problem at hand.

APPENDIX A PROOF OF LEMMA 7

The lemma essentially follows from Lemma 7 in [3]. A weighted hypergraph $(\mathcal{M}, \mathbf{w})$ is t -uniform if all hyperedges in $\mathcal{E} = \{e \in 2^{\mathcal{M}} : \mathbf{w}(e) > 0\}$ have size exactly t . In particular, a weighted graph satisfies this definition with $t = 2$. We then have the following lemma.

Lemma 9 ([3], Lemma 7). *Let $X_{\mathcal{M}}$ be a source defined on a t -uniform weighted hypergraph. For any $n \in \mathbb{N}$ and any function \mathbf{L} of $X_{\mathcal{M}}^n$, we have*

$$\sum_{i=1}^m I(X_i^n; \mathbf{L}) \leq t H(\mathbf{L}).$$

It should be clarified that Lemma 7 in [3] is stated only for hypergraphs with integer-valued weight functions \mathbf{w} . However, this restriction is not essential for the proof given in [3], so that it applies to any real-valued weight function \mathbf{w} just as well.

We will need the above lemma only for the case of graphical source models (i.e., $t = 2$).

To prove our Lemma 7, consider the given weighted graph $\mathcal{G} = (\mathcal{M}, \mathbf{w})$, with edge set $\mathcal{E} = \{e \in 2^{\mathcal{M}} : \mathbf{w}(e) > 0\}$, and the fundamental partition $\mathcal{P}^* = (A_1, \dots, A_k)$ of the corresponding source $X_{\mathcal{M}}$. From $X_{\mathcal{M}}$, we construct a closely related graphical source $\tilde{X}_{\mathcal{V}}$ on a vertex set \mathcal{V} , as described next.

For each pair of cells A_i, A_j of \mathcal{P}^* , with $i < j$, let $\mathcal{E}_{i,j}$ denote the set of edges of \mathcal{G} with one endpoint in A_i and the other in A_j . We further let \mathcal{E}_i be the set of edges of \mathcal{G} that are contained within A_i , $i = 1, 2, \dots, k$. Now, let $\{a_1, \dots, a_k\}$ and $\{a'_1, \dots, a'_k\}$ be two disjoint sets of size $k = |\mathcal{P}^*|$ each, and let $\mathcal{V} = \{a_1, \dots, a_k\} \cup \{a'_1, \dots, a'_k\}$. Define a weight function $\tilde{\mathbf{w}}$ on 2-subsets of \mathcal{V} as follows: for each pair of integers $i < j$, we set $\tilde{\mathbf{w}}(\{a_i, a_j\}) = \sum_{e \in \mathcal{E}_{i,j}} \mathbf{w}(e)$; and for $i = 1, 2, \dots, k$, set $\tilde{\mathbf{w}}(\{a_i, a'_i\}) = \sum_{e \in \mathcal{E}_i} \mathbf{w}(e)$. For all other 2-subsets \tilde{e} of \mathcal{V} , we set $\tilde{\mathbf{w}}(\tilde{e}) = 0$.

We take $\tilde{X}_{\mathcal{V}}$ to be a source defined on the weighted graph $(\mathcal{V}, \tilde{\mathbf{w}})$. To be precise, let ξ_e , $e \in \mathcal{E}$, be the random variables associated with the edges of the graphical source $X_{\mathcal{M}}$. In $\tilde{X}_{\mathcal{V}}$, we associate with each 2-subset (edge) \tilde{e} of \mathcal{V} , a random variable $\tilde{\xi}_{\tilde{e}}$ as below:

$$\tilde{\xi}_{\tilde{e}} = \begin{cases} (\xi_e : e \in \mathcal{E}_{i,j}) & \text{if } \tilde{e} = \{a_i, a_j\} \\ (\xi_e : e \in \mathcal{E}_i) & \text{if } \tilde{e} = \{a_i, a'_i\} \\ 0 & \text{otherwise.} \end{cases}$$

As usual, for any $v \in \mathcal{V}$, \tilde{X}_v refers to the random variable $(\xi_{\tilde{e}} : v \in \tilde{e})$. Observe, in particular, that $\tilde{X}_{a_i} = X_{A_i}$, for $i = 1, 2, \dots, k$.

Now, to complete the proof of Lemma 7, we note that for any function \mathbf{L} of $X_{\mathcal{M}}^n$, we have

$$\begin{aligned} \sum_{A \in \mathcal{P}^*} I(X_A^n; \mathbf{L}) &= \sum_{i=1}^k I(\tilde{X}_{a_i}^n; \mathbf{L}) \\ &\leq \sum_{v \in \mathcal{V}} I(\tilde{X}_v^n; \mathbf{L}) \\ &\leq 2H(\mathbf{L}) \end{aligned}$$

by Lemma 9 (with $t = 2$).

REFERENCES

- [1] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Trans. Inf. Theory*, vol. 50, pp. 3047–3061, Dec. 2004.
- [2] H. Tyagi, "Common information and secret key capacity," *IEEE Trans. Inf. Theory*, vol. 59, no. 9, pp. 5627–5640, Sep. 2013.
- [3] M. Mukherjee, N. Kashyap, Y. Sankarasubramanian, "On the public communication needed to achieve SK capacity in the multiterminal source model," arXiv:1507.02874.
- [4] A. C. Yao, "Some complexity questions related to distributed computing," in *Proc. 11th Annu. ACM Symp. Theory of Computing (STOC)*, 1979.
- [5] C. Chan and L. Zheng, "Mutual dependence for secret key agreement," in *Proc. 44th Annual Conference on Information Sciences and Systems (CISS)*, 2010.
- [6] S. El Rouayheb, A. Sprintson, and P. Sadeghi, "On coding for cooperative data exchange," in *Proc. 2010 IEEE Inf. Theory Workshop (ITW 2010)*, Cairo, Egypt, 6–8 Jan. 2010, pp. 1–5.

- [7] T. A. Courtade and R. D. Wesel, "Coded cooperative data exchange in multihop networks," *IEEE Trans. Inf. Theory*, vol. 60, no. 2, pp. 1136–1158, Feb. 2014.
- [8] T. A. Courtade and T. R. Halford, "Coded cooperative data exchange for a secret key," in *Proc. 2014 IEEE Int. Symp. Inf. Theory (ISIT 2014)*, Honolulu, Hawai'i, USA, June 29 – July 4, 2014, pp. 776–780.
- [9] T. A. Courtade and T. R. Halford, "Coded cooperative data exchange for a secret key," arXiv:1407.0333v1.
- [10] S. Nitinawarat, C. Ye, A. Barg, P. Narayan and A. Reznik, "Secret key generation for a pairwise independent network model," *IEEE Trans. Inf. Theory*, vol. 56, pp. 6482–6489, Dec. 2010.
- [11] S. Nitinawarat and P. Narayan, "Perfect omniscience, perfect secrecy and Steiner tree packing," *IEEE Trans. Inf. Theory*, vol. 56, no. 12, pp. 6490–6500, Dec. 2010.
- [12] C. Chan, A. Al-Bashabsheh and Q. Zhou, "Incremental and decremental secret key agreement," submitted to *2016 IEEE Int. Symp. Inf. Theory (ISIT 2016)*, Barcelona, Spain, July 10 – 15, 2016.
- [13] C. Chan, A. Al-Bashabsheh, J. Ebrahimi, T. Kaced and T. Liu, "Multivariate mutual information inspired by secret key agreement," in *Proc. of IEEE*, vol. 103, no. 10, pp. 1883–1913, Oct. 2015.
- [14] A. Schrijver, *Combinatorial Optimization: Polyhedra and Efficiency*, Volume A–C, Springer, 2004.
- [15] A. D. Wyner, "The common information of two dependent random variables," *IEEE Trans. Inf. Theory*, vol. IT-21, no. 2, pp. 163–179, Mar. 1975.
- [16] G. Xu, W. Liu and B. Chen, "Wyner's common information: Generalizations and a new lossy source coding interpretation," arXiv:1301.2237v1.